IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

UNITED STATES OF AMERICA,

v. **CRIMINAL NO. 2:16cr36**

GERALD ANDREW DARBY,

Defendant.

OPINION AND ORDER

This matter comes before the Court on the Motion to Compel Discovery filed by Gerald Andrew Darby ("Defendant"). ECF No. 30. For reasons set forth below, the Court **DENIES** the Motion. ECF No. 30.

I. BACKGROUND

A. The Playpen Investigation and Indictment of Defendant

The instant prosecution is the result of an FBI investigation into a website, Playpen, which facilitated the distribution of child pornography.[1] Playpen was hosted on the Tor network. The Tor network, which must be accessed through special software, provides increased anonymity to its users as compared with the traditional Internet. It does this by masking the Internet Protocol ("IP") addresses of those accessing and hosting websites on the network. IP addresses can be used to locate the physical addresses of computers. The Tor network masks IP addresses by diverting communications through a series of relay computers before sending them to their intended destinations. As a result of this diversion, websites can only see the IP address of the last computer through which a users' communications are routed. Likewise, users that visit

[1] A more detailed account of this investigation swith citations to the record may be found in the Court's Opinion and Order denying Defendant's First and Second Motions to Suppress. ECF No. 31.

websites hosted on the Tor network cannot determine the IP addresses of the servers hosting the websites because the information from these websites is routed through intermediaries. Websites hosted on the Tor network are known as hidden services.

The government was able to locate the server where Playpen was hosted as well as the individual who administered the site. The government made a copy of the website and hosted it on a server located in a government facility in the Eastern District of Virginia. FBI agents sought and obtained a lawful search warrant that allowed them to deploy a Network Investigative Technique, or "NIT," against the computers of those individuals who registered with Playpen and then logged into the site. The NIT would allow the FBI to circumvent the anonymity of the Tor network and identify individuals who visited Playpen. The workings of the NIT will be described in more detail below. In short, the NIT bypassed the security features of the Tor browser and instructed the target computers to send certain identifying information to a government server. The warrant allowed the NIT to transmit the following information: the computer's IP address, a unique identifier generated by the NIT, the type of operating system running on the computer, information about whether the NIT had previously been delivered to the computer, the computer's host name, the user name of the computer's operating system, and the computer's media access control ("MAC") address. See Warrant Appl., Attach. B, ECF No. 16-1 at 2.

According to Defendant's own briefing in support of his First Motion to Suppress, on or about February 27, 2015, the Playpen website sent the instructions for the NIT to his computer. Def.'s First Mot. to Suppress, ECF No. 15 at 10. The FBI issued an administrative subpoena to Defendant's Internet Service Provider, Verizon, demanding information associated with the IP address obtained by the NIT from his computer. Id. at 10–11. Verizon provided Defendant's name, subscriber information, and address to the government. Id. On January 4, 2016, a warrant to search Defendant's home was issued by Magistrate Judge Robert J. Krask. Id. at 11. FBI agents searched Defendant's home on January 7, 2016 and seized computers, hard drives, cell phones, tablets, video game systems, and other property. Id. According to the government, Defendant was present during the search and agreed to be interviewed. Gov't's Resp. to Def.'s First Mot. to Suppress, ECF No. 16 at 7. During this interview Defendant admitted to downloading sexually explicit images of minors for the past three to four years. Id. The government also relates that forensic analysis found that Defendant possessed 1,608 images and 298 videos of child pornography. Id.

On March 10, 2016 a grand jury returned an indictment charging Defendant with five counts of Receipt of Images of Minors Engaging in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(2) and three counts of Possession of Images of Minors Engaging in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(4)(B). ECF No. 1. Defendant filed two Motions to Suppress, which this Court denied. See Opinion and Order, ECF No. 31. On June 2, 2016, Defendant filed the instant Motion to Compel Discovery. ECF No. 30. The government responded on June 16, 2016. Gov't's Resp. to Def.'s Mot. to Compel (Gov't's Resp.), ECF No. 37. On July 5, 2016, the Court held a hearing on the Motion. Hr'g, ECF No. 46. This was a joint hearing at which counsel for another defendant located through the government's operation of Playpen appeared to argue the instant Motion to Compel and a nearly identical Motion to Compel filed by his client.[2] Two witnesses testified at the hearing: Defendant called Dr. Christopher Soghoian, a technologist; and the government called FBI Special Agent Daniel

[2] The other defendant's case is United States v. Hunter Vaughan Eure, No. 2:16cr43 (E.D.Va.). Both Mr. Eure and Mr. Darby are represented by the Federal Public Defender's Office and have submitted nearly identical Motions to Suppress and Motions to Compel Discovery. The undersigned gave counsel for Mr. Darby the opportunity to speak at the hearing and counsel declined. The testimony at the hearing is part of the record of both cases.

Alfin. Hr'g, ECF No. 46.

B. The Network Investigative Technique ("NIT")

With the Motion to Compel, Defendant asks this Court to order "the government to provide the source code or programming code for the NIT it used to search [Defendant's] computer." Def.'s Mot. to Compel Disc. at 1. Defendant wants the government to provide what he refers to as "the payload, exploit, payload generator, and server component," which, collectively, he claims constitute the "full source code" of the NIT. See Decl. of Vlad Tsyrklevich ("Tsyrklevich Decl.") ¶ 4, ECF No. 30-1, Ex. A. Although the government has at times disputed whether the source code of the NIT technically constitutes all of these components, see Gov't's Resp. at 10 (claiming that Defendant "fundamentally misunderstand[s]" the NIT's basic structure), there is no disagreement concerning what the government has provided or offered to provide to Defendant or about what Defendant would like in addition to these disclosures. Any disagreements about what constitutes the source code of the NIT are purely semantic and of no practical significance.

In order to understand what Defendant would like the government to turn over, a brief description of the operation of the NIT is necessary.[3] As recounted above, for a brief period the government ran Playpen, a hidden service on the Tor network, from a server located in Virginia. The FBI obtained a warrant allowing the government to perform a limited search of the computers of any individual who registered and then logged into Playpen. When an individual logged into Playpen, the site assigned each individual a unique identifier that allowed the government to connect the users identified by the NIT with the website activity of that individual. See Gov't's Resp. at 11–12. The code that generated this identifier is the main

[3] Support for this account may be found in the briefing on the present motion, the hearing held on the present motion, and the briefing in United States v. Eure, 2:16cr43 (E.D.Va.), another Playpen case before the undersigned.

component of what Defendant refers to as the "payload generator."

Ultimately, Playpen sent to each individual's computer what Defendant refers to as the payload, Tsyrklevich Decl. ¶ 4, and the government refers to, in accordance with the language used in the warrant application, as "the computer instructions . . . that gathered [Defendant's] identifying information . . . ", Gov't's Resp. at 10. According to Defendant's experts, Playpen first sent to his computer an "exploit" that undermined the features of the Tor browser such that the payload could be placed on Defendant's computer. See Tsyrklevich Decl. ¶¶ 4–6. The government disputes that the exploit is part of the NIT. Gov't's Resp. at 10. However, the government concedes that there is an "exploit" that allowed the government to "deliver" computer instructions to Defendant's computer. See Gov't's Resp. to Def.'s Mot. to Compel, United States v. Hunter Vaughan Eure, 2:16cr43 (E.D.Va.), ECF No. 32 at 10–11. After the computer instructions or payload was placed on Defendant's computer, it instructed his computer to send information—including Defendant's IP address and the unique identifier generated by Playpen—to a government server. This server Defendant refers to as the "server component" or "data preservation component" of the NIT. Tsyrklevich Decl. ¶¶ 4–6. Defendant would like to review the government's servers and the data stored within them.

The government has already turned over some of what Defendant requests. Additionally, it has provided material—or offered the opportunity to Defendant to inspect certain evidence—that it believes would allay Defendant's concerns about the operation of the NIT. The government has provided Defendant with the computer instructions it placed on his computer, which Defendant refers to as the payload. The government has also provided the data that were sent from Defendant's computer to the government server. These data are stored in a PCAP file, which has been docketed in readable form. Decl. of Special Agent Daniel Alfin ("Second Alfin

Decl."), ECF No. 45, Ex. 1A. The government has offered Defendant the opportunity to run a copy of the payload on Defendant's computer. It has offered Defendant the opportunity to otherwise inspect his computer. It has offered to provide a copy of the Playpen website as it existed when the government administered it. While administering Playpen, the government recorded the activity of each visitor to the site. The government has offered Defendant those records that track the username that the government alleges was Defendant's.

The government will not turn over the exploit or the code that generated the unique identification codes for each visitor to Playpen. The government will not allow Defendant access to its servers.

II. LEGAL PRINCIPLES

Defendant brings this Motion under Federal Rule of Criminal Procedure 16(d), which gives this Court the power to issues orders to enforce Rule 16.[4] Under Rule 16, "[u]pon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies of portions of any of these items, if the item is within the government's possession, custody, or control and . . . the item is material to preparing a defense . . . ." Fed. R. Crim. P. 16(a)(1)(E). A "defense" in the context of Rule 16 "means the defendant's response to the government's case in chief." United States v. Armstrong, 517 U.S. 456, 462 (1996).

The Fourth Circuit has said that "[e]vidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." United States v.

[4] The government's obligations under Rule 16 are greater than its obligations under Brady v. Maryland, 373 U.S. 83 (1963), which rests upon due process consideration, and provides a minimum amount of pretrial discovery granted in criminal cases" United States v. Caro, 587 F.3d 608, 620 (4th Cir. 2010) (citing United States v. Baker, 453 F.3d 419, 424 (7th Cir. 2006) ("Rule 16 . . . is broader than Brady.")).

Caro, 587 F.3d 608, 621 (4th Cir. 2010) (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)). It has also said, in the same paragraph of the same opinion, that to establish materiality, a defendant must present a court with "some indication" that the evidence sought would "significantly . . . alter the burden of proof in his favor." Id. (quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975)).[5] Whatever the formulation of the standard for materiality—whether there must be a strong indication that the evidence will play an important role or some indication that the evidence will significantly alter the burden of proof—it is not enough for a defendant to present "a general description of the information sought []or conclusory allegations of materiality." Id. (quoting United States v. Mandel, 914 F.2d 1215, 1219 (9th Cir. 1990)). A defendant "must present facts that would tend to show that the government is in possession of information helpful to the defense." Id. (quoting Mandel, 914 F.2d at 1219).

In addition to arguing that Defendant fails to show that the evidence he seeks is material, the government also argues that the evidence, particularly the exploit, is protected by the law enforcement privilege. The Fourth Circuit has not directly addressed the law enforcement privilege, although courts in the Eastern District of Virginia have.[6] The circuits that have addressed the issue have set out a basic framework for evaluating the privilege.

It is the burden of the party asserting the privilege, in this case the federal government, to show that the privilege applies. In re The City of New York, 607 F.3d 923, 948 (2d Cir. 2010) (citing In re Sealed Case, 856 F.2d 268, 271–72 (D.C. Cir. 1998)). The government must show

[5] In a footnote, the Fourth Circuit indicated that it may be adopting this latter standard. Caro, 587 F.3d at 621 n.15.
[6] Judge Henry Morgan, who serves with the undersigned in the Norfolk Division of the Eastern District of Virginia, has written an excellent opinion addressing whether the law enforcement privilege applies to the information sought by another defendant indicted as a result of the NIT deployed by the FBI through Playpen. United States v. Matish, No. 4:16cr16, 2016 WL 3545776, at *5–9 (E.D. Va. June 23, 2016). Judge Morgan's opinion also addresses whether Rule 16 required the government to disclose the exploit. Id. He found both that Rule 16 did not require disclosure of the exploit and that the exploit was protected by the law enforcement privilege. Id.

that the evidence contains

> (1) information pertaining to law enforcement techniques and procedures, (2) information that would undermine the confidentiality of sources, (3) information that would endanger witness and law enforcement personnel, (4) information that would undermine the privacy of individuals involved in an investigation, or (5) information that would seriously impair the ability of a law enforcement agency to conduct future investigations.

Id. (internal citations and quotations omitted). The privilege is not absolute. Id. If the government establishes that the privilege applies, a district court then "must balance the public interest in nondisclosure against 'the need of a particular litigant for access to the privileged information.'" Id. (citing In re Sealed Case, 856 F.2d at 272).

III. ANALYSIS

This opinion will address why Defendant is not entitled to each particular piece of information he seeks. However, the chief shortcoming of Defendant's Motion applies to all of his requests. Defendant invents a variety of scenarios whereby the information he seeks about the operation of the NIT might aid him in developing a defense. Defendant has not used any of the information that the government has provided to him or offered to provide him in order to establish a factual basis for these scenarios. As a result, the Court does not have before it any evidence that the information sought would aid this Defendant. Furthermore, the scenarios, mostly, are not drawn to any particular feature of the NIT used by the government and would apply to any NIT deployed by means of an exploit. In short, all Defendant places before the Court are stories about how a generic defendant located by means of a generic NIT might need the information sought in order to develop his or her defense. This is not enough to require disclosure under the standards established by the Fourth Circuit in Caro.

Defendant seeks disclosure of what he calls the payload generator. One function of this payload generator, according to Defendant, is to generate a unique identification number for each user that logged into Playpen. It is the code that generates these unique identifiers that Defendant seeks. Although the government disputes that a payload generator was part of the NIT, it acknowledges that it created these unique identifiers and matched them to each username that logged into Playpen. The unique identifier was sent to each user's computer and then sent back to the government along with information about the computer. The government maintained a record of all activity that took place on Playpen while it ran the site. Using the unique identifiers sent back by the NIT, the government was able to match its logs of the activity on Playpen with the individuals identified by the NIT.

Defendant claims that he needs the code that generated the unique identifiers so that he can confirm that the code did not create any duplicate identifiers. The government has submitted a declaration from Special Agent Alfin wherein he states that there were no duplicates among the identifiers sent back to the government by the computers upon which the NIT was placed. Decl. of Special Agent Daniel Alfin ("First Alfin Decl.") ¶¶ 26–27, ECF No. 37-1. Defendant argues that he should not have to rely on the assurances of the government that its code worked as it should. Although there is some merit to this contention, Defendant has not submitted any evidence in support of his contention that there may have been duplicate identifiers or explained why, even if there were, it would aid in his defense.

The government located Defendant based on the IP address sent to the government by the NIT from his computer. The NIT was only placed on the computers of individuals who logged into Playpen. The code assigned to Defendant by Playpen played no role in identifying him. Even if the identifier sent to his computer was a duplicate, it would not affect the government's evidence that Defendant logged into Playpen. In fact, Defendant, in his briefing in support of his First Motion to Suppress, acknowledges that the NIT was placed on his computer. ECF No. 15 at

10–11. Disclosure of the code used to generate the unique identifier would not affect this aspect of the government's case in chief.

The government used the identifiers to match the individuals located by the NIT with the usernames of those that logged into Playpen. The government has offered to provide Defendant with the activity records of the username it has associated with him. Defendant could have used these records to support his claim that there were duplicate identifiers. But Defendant has put forth nothing but speculation that such duplicates might have existed. This is not enough under Caro to mandate disclosure by the government.

Defendant also seeks disclosure of the exploit that was used to undermine the security features of the Tor browser such that the government was able to place on his computer the NIT instructions. These instructions gathered identifying information from his computer and sent this information to a government server. It is important to note that the government has provided the NIT instructions and the data stream that was sent from his computer. It has also offered Defendant the opportunity to run these instructions on his computer to confirm that the NIT did exactly was the government said it did in the warrant application. Defendant's concerns about the operation of and data collected by the NIT have been addressed by these disclosures.

Nevertheless, Defendant claims that he still needs the code for the exploit. His arguments for why he needs the exploit are all premised on the FBI lying to him about its operation. He argues that he needs the exploit because the exploit might have "executed additional functions outside of the NIT warrant." Tsyrkelich Decl. at 3. Special Agent Alfin has submitted a sworn declaration refuting this contention. See First Alfin Decl. ¶¶ 10-11 (asserting that the exploit merely allowed the NIT instructions to be placed on Defendant's computer). Defendant has not submitted any evidence to refute this contention. He merely says that he should not have to trust the sworn statements of government agents. However, in order to be entitled to discovery under Caro, he must show that the information sought is material and speculations not supported by any evidence are not enough to show that the information sought is material.

Defendant also argues the he needs to examine the code for the exploit because the exploit might have altered the security features of his computer. Other individuals might then have placed child pornography on his compromised computer.[7] Again, Special Agent Alfin has stated in his declaration that the exploit does not weaken the security features of the computers against which it is deployed. First Alfin Decl. ¶ 14. Again, Defendant says that he should not have to rely on the assurances of government agents. Again, Defendant submits no evidence that the security features of his computer were altered. The government has offered Defendant the opportunity to inspect his computer for signs that its security features were compromised and for signs that it was later hacked. Yet, Defendant still presents no evidence in support of his hypothetical. Absent in evidence in support of his hypothetical, he is not entitled to disclosure of the exploit.

Additionally, the government has asserted that the law enforcement privilege applies because disclosure of the exploit would be harmful to the public interest. The undersigned has reviewed a confidential brief submitted by the government. Based on this briefing, the Court finds that the exploit is protected by the law enforcement privilege. Defendant has not put forth any credible argument as to why he needs the exploit. Accordingly, the Court also finds that the public interest in nondisclosure outweighs Defendant's need for the information.

Finally, Defendant seeks disclosure of the server component of the NIT. As noted earlier, the government has already provided to Defendant—and docketed with the Court—the data

[7] This story, however implausible, might explain away the child pornography found on Defendant's computer. It does not explain what Defendant was doing on Playpen.

stream sent by Defendant's computer to the government's server. It has also offered Defendant the opportunity to run the NIT on his computer to confirm that the data provided by the government matches the data produced by running the NIT on his computer. Access to the government's servers would do nothing to aid Defendant in the preparation of his defense. Accordingly, Defendant is not entitled under Caro to examine the government's servers.

IV. CONCLUSION

For the reasons stated above, the Court **DENIES** Defendant's Motion to Compel Discovery. ECF No. 30.

The Clerk is **DIRECTED** to forward a copy of this Order to all Counsel of Record.

IT IS SO ORDERED.

/s/
Robert G. Doumar
Senior United States District Judge
UNITED STATES DISTRICT JUDGE

Norfolk, VA
August 12, 2016